Network Working Group
Request for Comments: 2867
Category: Informational
Updates: 2866

G. Zorn
Cisco Systems, Inc.
B. Aboba
Microsoft Corporation
D. Mitton
Nortel Networks

June 2000

RADIUS Accounting Modifications for Tunnel Protocol Support

Status of this Memo

Copyright Notice

Abstract

This document defines new RADIUS accounting Attributes and new values for the existing Acct-Status-Type Attribute [1] designed to support the provision of compulsory tunneling in dial-up networks.

Specification of Requirements

In this document, the key words "MAY", "MUST, "MUST NOT", "optional", "recommended", "SHOULD", and "SHOULD NOT", are to be interpreted as described in [2].

1. Introduction

Many applications of tunneling protocols such as PPTP [5] and L2TP [4] involve dial-up network access. Some, such as the provision of secure access to corporate intranets via the Internet, are characterized by voluntary tunneling: the tunnel is created at the request of the user for a specific purpose. Other applications involve compulsory tunneling: the tunnel is created without any action from the user and without allowing the user any choice in the matter, as a service of the Internet service provider (ISP). Typically, ISPs providing a service want to collect data regarding that service for billing, network planning, etc. One way to collect usage data in dial-up networks is by means of RADIUS Accounting [1]. The use of RADIUS Accounting allows dial-up usage data to be collected at a central location, rather than stored on each NAS.

In order to collect usage data regarding tunneling, new RADIUS attributes are needed; this document defines these attributes. In addition, several new values for the Acct-Status-Type attribute are proposed. Specific recommendations for, and examples of, the application of this attribute for the L2TP protocol can be found in RFC 2809.

2. Implementation Notes

Compulsory tunneling may be part of a package of services provided by one entity to another. For example, a corporation might contract with an ISP to provide remote intranet access to its employees via compulsory tunneling. In this case, the integration of RADIUS and tunnel protocols allows the ISP and the corporation to synchronize their accounting activities so that each side receives a record of the user's resource consumption. This provides the corporation with the means to audit ISP bills.

In auditing, the User-Name, Acct-Tunnel-Connection, Tunnel-Client-Endpoint and Tunnel-Server-Endpoint attributes are typically used to uniquely identify the call, allowing the Accounting-Request sent by the NAS to be reconciled with the corresponding Accounting-Request sent by the tunnel server.

When implementing RADIUS accounting for L2TP/PPTP tunneling, the Call-Serial-Number SHOULD be used in the Acct-Tunnel-Connection attribute. In L2TP, the Call-Serial-Number is a 32-bit field and in PPTP it is a 16-bit field. In PPTP the combination of IP Address and Call-Serial-Number SHOULD be unique, but this is not required. In addition, no method for determining the Call-Serial-Number is specified, which leaves open the possibility of wrapping after a reboot.

Note that a 16-bit Call-Serial-Number is not sufficient to distinguish a given call from all other calls over an extended time period. For example, if the Call-Serial-Number is assigned monotonically, the NAS in question has 96 ports which are continually busy and the average call is of 20 minutes duration, then a 16-bit Call-Serial-Number will wrap within 65536/(96 * 3 calls/hour * 24 hours/day) = 9.48 days.

3. New Acct-Status-Type Values

3.1. Tunnel-Start

Value

9

Description

This value MAY be used to mark the establishment of a tunnel with another node. If this value is used, the following attributes SHOULD also be included in the Accounting-Request packet:

User-Name (1)
NAS-IP-Address (4)
Acct-Delay-Time (41)
Event-Timestamp (55)
Tunnel-Type (64)
Tunnel-Medium-Type (65)
Tunnel-Client-Endpoint (66)
Tunnel-Server-Endpoint (67)
Acct-Tunnel-Connection (68)

3.2. Tunnel-Stop

Value

10

Description

This value MAY be used to mark the destruction of a tunnel to or from another node. If this value is used, the following attributes SHOULD also be included in the Accounting-Request packet:

User-Name (1)
NAS-IP-Address (4)
Acct-Delay-Time (41)
Acct-Input-Octets (42)
Acct-Output-Octets (43)
Acct-Session-Id (44)
Acct-Session-Time (46)
Acct-Input-Packets (47)
Acct-Output-Packets (48)
Acct-Terminate-Cause (49)
Acct-Multi-Session-Id (51)
Event-Timestamp (55)
Tunnel-Type (64)
Tunnel-Medium-Type (65)
Tunnel-Client-Endpoint (66)
Tunnel-Server-Endpoint (67)
Acct-Tunnel-Connection (68)
Acct-Tunnel-Packets-Lost (86)

3.3. Tunnel-Reject

Value

11

Description

This value MAY be used to mark the rejection of the establishment of a tunnel with another node. If this value is used, the following attributes SHOULD also be included in the Accounting-Request packet:

User-Name (1)
NAS-IP-Address (4)
Acct-Delay-Time (41)
Acct-Terminate-Cause (49)
Event-Timestamp (55)
Tunnel-Type (64)
Tunnel-Medium-Type (65)
Tunnel-Client-Endpoint (66)
Tunnel-Server-Endpoint (67)
Acct-Tunnel-Connection (68)

3.4. Tunnel-Link-Start

Value

12

Description

This value MAY be used to mark the creation of a tunnel link. Only some tunnel types (e.g., L2TP) support multiple links per tunnel. This Attribute is intended to mark the creation of a link within a tunnel that carries multiple links. For example, if a mandatory tunnel were to carry M links over its lifetime, 2(M+1) RADIUS Accounting messages might be sent: one each marking the initiation and destruction of the tunnel itself and one each for the initiation and destruction of each link within the tunnel. If only a single link can be carried in a given tunnel (e.g., IPsec in the tunnel mode), this Attribute need not be included in accounting packets, since the presence of the Tunnel-Start Attribute will imply the initiation of the (only possible) link.

If this value is used, the following attributes SHOULD also be included in the Accounting-Request packet:

User-Name (1)
NAS-IP-Address (4)
NAS-Port (5)
Acct-Delay-Time (41)
Event-Timestamp (55)
Tunnel-Type (64)
Tunnel-Medium-Type (65)
Tunnel-Client-Endpoint (66)
Tunnel-Server-Endpoint (67)
Acct-Tunnel-Connection (68)

3.5. Tunnel-Link-Stop

Value

13

Description

This value MAY be used to mark the destruction of a tunnel link. Only some tunnel types (e.g., L2TP) support multiple links per tunnel. This Attribute is intended to mark the destruction of a link within a tunnel that carries multiple links. For example, if a mandatory tunnel were to carry M links over its lifetime, 2(M+1) RADIUS Accounting messages might be sent: one each marking the initiation and destruction of the tunnel itself and one each for the initiation and destruction of each link within the tunnel. If only a single link can be carried in a given tunnel (e.g., IPsec in the tunnel mode), this Attribute need not be included in accounting packets, since the presence of the Tunnel-Stop Attribute will imply the termination of the (only possible) link.

If this value is used, the following attributes SHOULD also be included in the Accounting-Request packet:

User-Name (1)
NAS-IP-Address (4)
NAS-Port (5)
Acct-Delay-Time (41)
Acct-Input-Octets (42)
Acct-Output-Octets (43)
Acct-Session-Id (44)
Acct-Session-Time (46)
Acct-Input-Packets (47)

Acct-Output-Packets (48)
Acct-Terminate-Cause (49)
Acct-Multi-Session-Id (51)
Event-Timestamp (55)
NAS-Port-Type (61)
Tunnel-Type (64)
Tunnel-Medium-Type (65)
Tunnel-Client-Endpoint (66)
Tunnel-Server-Endpoint (67)
Acct-Tunnel-Connection (68)
Acct-Tunnel-Packets-Lost (86)

3.6. Tunnel-Link-Reject

Value

14

Description

This value MAY be used to mark the rejection of the establishment of a new link in an existing tunnel. Only some tunnel types (e.g., L2TP) support multiple links per tunnel. If only a single link can be carried in a given tunnel (e.g., IPsec in the tunnel mode), this Attribute need not be included in accounting packets, since in this case the Tunnel-Reject Attribute has the same meaning.

If this value is used, the following attributes SHOULD also be included in the Accounting-Request packet:

User-Name (1)
NAS-IP-Address (4)
Acct-Delay-Time (41)
Acct-Terminate-Cause (49)
Event-Timestamp (55)
Tunnel-Type (64)
Tunnel-Medium-Type (65)
Tunnel-Client-Endpoint (66)
Tunnel-Server-Endpoint (67)
Acct-Tunnel-Connection (68)

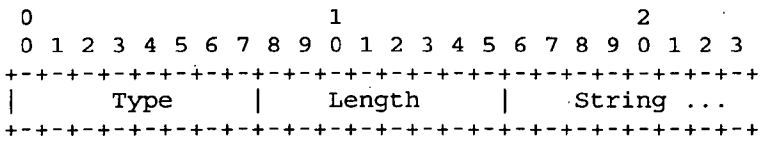
4. Attributes

4.1. Acct-Tunnel-Connection

Description

This Attribute indicates the identifier assigned to the tunnel session. It SHOULD be included in Accounting-Request packets which contain an Acct-Status-Type attribute having the value Start, Stop or any of the values described above. This attribute, along with the Tunnel-Client-Endpoint and Tunnel-Server-Endpoint attributes [3], may be used to provide a means to uniquely identify a tunnel session for auditing purposes.

A summary of the Acct-Tunnel-Connection Attribute format is shown below. The fields are transmitted from left to right.



Type

68 for Acct-Tunnel-Connection

Length

>= 3

String

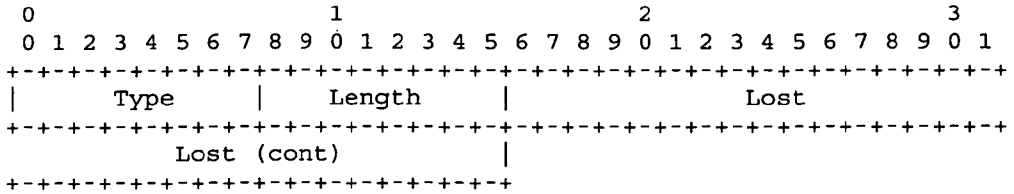
The format of the identifier represented by the String field depends upon the value of the Tunnel-Type attribute [3]. For example, to fully identify an L2TP tunnel connection, the L2TP Tunnel ID and Call ID might be encoded in this field. The exact encoding of this field is implementation dependent.

4.2. Acct-Tunnel-Packets-Lost

Description

This Attribute indicates the number of packets lost on a given link. It SHOULD be included in Accounting-Request packets which contain an Acct-Status-Type attribute having the value Tunnel-Link-Stop.

A summary of the Acct-Tunnel-Packets-Lost Attribute format is shown below. The fields are transmitted from left to right.



Type

86 for Acct-Tunnel-Packets-Lost

Length

6

Lost

The Lost field is 4 octets in length and represents the number of packets lost on the link.

5. Table of Attributes

The following table provides a guide to which attributes may be found in Accounting-Request packets. No tunnel attributes should be found in Accounting-Response packets.

Request	#	Attribute
0-1	64	Tunnel-Type
0-1	65	Tunnel-Medium-Type
0-1	66	Tunnel-Client-Endpoint
0-1	67	Tunnel-Server-Endpoint
0-1	68	Acct-Tunnel-Connection
0	69	Tunnel-Password
0-1	81	Tunnel-Private-Group-ID
0-1	82	Tunnel-Assignment-ID
0	83	Tunnel-Preference
0-1	86	Acct-Tunnel-Packets-Lost

The following table defines the meaning of the above table entries.

0	This attribute MUST NOT be present in packet.
0+	Zero or more instances of this attribute MAY be present in packet.
0-1	Zero or one instance of this attribute MAY be present in packet.

6. Security Considerations

By "sniffing" RADIUS Accounting packets, it might be possible for an eavesdropper to perform a passive analysis of tunnel connections.

7. References

[1] Rigney, C., "RADIUS Accounting", RFC 2866, June 2000.

[2] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[3] Zorn, G., Leifer, D., Rubens, A., Shriver, J., Holdrege, M. and I. Goyret, "RADIUS Attributes for Tunnel Protocol Support", RFC 2868, June 2000.

[4] Townsley, W., Valencia, A., Rubens, A., Pall, G., Zorn, G. and B. Palter, "Layer Two Tunneling Protocol "L2TP"", RFC 2661, August 1999.

[5] Hamzeh, K., Pall, G., Verthein, W., Taarud, J., Little, W. and G. Zorn, "Point-to-Point Tunneling Protocol (PPTP)", RFC 2637, July 1999.

8. Acknowledgments

Thanks to Aydin Edguer, Ly Loi, Matt Holdrege and Gurdeep Singh Pall for salient input and review.

9. Authors' Addresses

Questions about this memo can be directed to:

Glen Zorn
Cisco Systems, Inc.
500 108th Avenue N.E., Suite 500
Bellevue, Washington 98004
USA

Phone: +1 425 438 8218
FAX: +1 425 438 1848
EMail: gwz@cisco.com

Dave Mitton
Nortel Networks
880 Technology Park Drive
Billerica, MA 01821

Phone: +1 978 288 4570
Fax: +1 978 288 3030
EMail: dmitton@nortelnetworks.com

Bernard Aboba
Microsoft Corporation
One Microsoft Way
Redmond, Washington 98052

Phone: +1 425 936 6605
Fax: +1 425 936 7329
EMail: aboba@internaut.com

10. Full Copyright Statement

Acknowledgement

Funding for the RFC Editor function is currently provided by the Internet Society.